

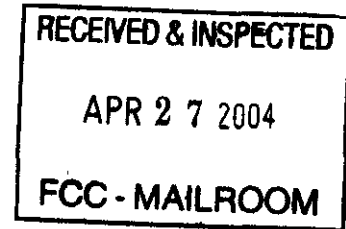


WAYNE E BENNETT
SUPERINTENDENT

DOCKET FILE COPY ORIGINAL

NEW YORK STATE POLICE
BLDG 22, 1220 WASHINGTON AVE
ALBANY, NEW YORK 12226-2252

April 12, 2004



Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

Re: RM-10865/DA No. 04-700 --
Comments on the CALEA Petition for Rulemaking

Dear Secretary Dortch:

The New York State Police submits these comments on the U.S. Department of Justice's ("DOJ"), Federal Bureau of Investigation's ("FBI"), and U.S. Drug Enforcement Administration's ("DEA") Joint Petition ("Petition") filed on March 10, 2004, before the Federal Communications Commission ("FCC") requesting that the FCC resolve, on an expedited basis, various critically important issues arising from the implementation of the Communications Assistance for Law Enforcement Act ("CALEA").

It is vitally important, and consistent with Congress's intent in enacting CALEA, that the FCC initiate a rulemaking proceeding and adopt the rules proposed by the DOJ, FBI, and DEA in the above Petition. Congress enacted CALEA in 1994 to insure that law enforcement has the ability to conduct authorized wiretaps in the future as technologies changed. Since 1994, many new communications technologies have arisen, including broadband Internet access, voice over IP telephony ("VoIP"), push-to-talk digital dispatch services, and other packet mode services. These services, currently used by millions of American citizens, pose a great challenge to state and local law enforcement in that many such providers of these communications services have failed to voluntarily adopt currently available CALEA intercept solutions. Thus, law enforcement has been thwarted in its attempts to implement lawfully authorized surveillance intercepts. Voluntary industry compliance with CALEA does not work.

With the convergence of the network infrastructure many new services and features have been made available to the general public, as well as, the criminal element. These services and features have become co-mingled and their interception has become difficult if not impossible and/or too expensive to attempt. Currently, the ability of the criminal element to use their computer and/or Voice over Internet Protocol (VoIP) or Voice over Packet (VOP) broadband services, in place of traditional telephones, to place local, long distance and worldwide calls has made the interception of these communications impossible. Providers or manufacturers have not made access to these communications available to Law Enforcement Agencies (LEA).

No. of Copies rec'd _____
List ASCDE _____

When the criminal element is aware that they can operate without fear of detection, they will migrate to these new technologies. This was demonstrated with the Nextel digital dispatch service known as "push-to-talk", which the FCC recognized to be covered under CALEA. We are now facing the same issue with regard to Verizon Wireless' new digital dispatch service. They have released this same service to the public without the ability of LEA's to access the communications occurring. Verizon Wireless disregarded the FCC's ruling on digital dispatch services sighting that a CALEA compliant solution did not exist at the time they released this service. When the criminal element realizes that LEA's do not have access to communications while using Verizon Wireless' or any other carrier's digital dispatch service, they will move to those services in an attempt to avoid detection.

There are other service providers both in the telecommunications industry and the information services industry who have released or are poised to release features and services that are either covered under CALEA or that should be covered under CALEA, without having provided a CALEA compliant delivery function. They have no regard for LEA's ability to conduct lawfully authorized electronic surveillance of these services and features and choose to delay compliance. The ability of a cellular telephone to be used to communicate other packet mode communications besides circuit-mode voice and an LEA's inability to intercept these communications is of great concern to law enforcement. It is not unreasonable to think that the criminal element will move to the use of VoIP via their cellular telephone or wireless PDA when connected to a local "hotspot" (wireless Internet Access Point). If this occurs and the FCC has not ruled that these types of communications are covered under CALEA, Law Enforcement's ability to conduct lawfully authorized surveillance of these services or features will be dramatically affected or none existent.

Furthermore, state and local law enforcement do not have the financial or personnel resources to develop costly *ad hoc* surveillance solutions for each new communications service. Nor should they have to under the current law. For all equipment, services, and facilities deployed after January 1, 1995, Congress, through CALEA, expressly passed the burden of designing and paying for such surveillance solutions onto the telecommunications carriers themselves.

Given the importance of the issues discussed above, it is important that the FCC promptly act upon the Petition and commence a rulemaking proceeding adopting the DOJ's, DEA's and FBI's proposed rules.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Wayne E. Bennett", with a long horizontal flourish extending to the right.

Wayne E. Bennett
Superintendent